*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. 1 (Mar – Apr. 2015), PP 28-36*
*www.iosrjournals.org*

# Blind Signature Scheme Based On Elliptical Curve Cryptography (ECC)

Preeti Singh[1]

*(M.tech(scholar),Computer Science And Engineering,Azad Institute Of Engineering &Technology,*

***Abstract:*** *Blind signature is a concept to ensure anonymity of e-coins. Untracebility and unlinkability are ttwo main properties of real coins and should also be mimicked electronicaly. A user has fulfill above two properties of blind signature for permission to send an e-coins. During the last few years, asymmetric cryptography based on curve based cryptography have becomes very popular, especially for embedded applications. Elliptical curves cryptography (CC) are the special case of elliptical curves (EC). EC operand size is only a fraction of the EC operand Size. EC Cryptography needs a group order of size atleast* $2^{160}$*. In Particular for a cuve of genus two field* $F_{q-}$*with p long operands. Which is much better than the RSA using 1024 bit key length. The elliptic curve is best suited for the resource constraint environment s. It uses lesser key and provides more secure transmission of data.*

***Index Terms:*** *Hyperelliptic curve cryptography, proxy signature, Blind signature, symmetric key cryptography, Asymmetric cryptography*.

## I. Introduction

The study of information hiding and verification is called Cryptography. It includesthe protocols, algorithms and strategies to securely and consistently prevents access of sensitive information from unauthorised person and enable verifiability of every component in a communication. Cryptanalysis is the study of how to circumvent the use of cryptography for unintended recipients or called as code breaking. Cryptography and cryptanalysis are sometimes grouped together under the umbrella coined cryptology, encompassing the entire subject. In practice, cryptography is often used to refer the field as a whole, especially as an applied science. Cryptography is an interdisciplinary subject, drawing from several fields. Before the time of computers. This includes topics from information theory, number theory, statistics, computational complexity and combinatorics. This is also a branch of engineering but an unusual one as it must deal with malevolent opposition, intelligent and active.

### A. History of cryptography

Until a few decades ago, the information collected by an organization was stored on physical files. The confidentiality of the files was achieved by restricting the access to a few authorized and trusted people in th organization, In the same way, only a few authorized people were allowed to change the contents of files. The availability was achieved by designating at least one person who would have access to the files at all times.

With the advent of computers information storage are now in electronic media. Instead of being stored on physical media, it was stored in computers. The three security requirements, however did not change. The files stored in computers required confidentiality, integrity and availability. The implementation of these requirements however is different and more challenging. Some security mechanisms can be implemented using cryptography. Cryptography used to refer to the science and art of transforming messages to make them secure and protect from attacks. Although in past cryptography referred only to the encryption and decryption of messages using secret keys, now a days it is defined as involving three distinct mechanisms: symmetric key cryptography and asymmetric key cryptography.

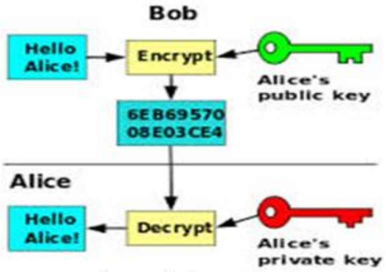

**Figure:** - encryption and decryption in cryptography

### B. Symmetric key cryptography

An entity Alice can send a message to another entity Bob over an insecure channel with the assumption that an adversary Eve cannot understand the contents of the message by simply eavesdropping over the channel. The original message form Alice to Bob is called plaintext: the message that is sent through the channel is called the ciphertext. To create the ciphertext from the plaintext, Alice uses an encryption algorithm and a shared secret key. To create the paintext from ciphertext. Bob uses a decryption algorithm and the same secret key. A key is a set of values(numbers) that the encryption/decryption algorithms use for operations.

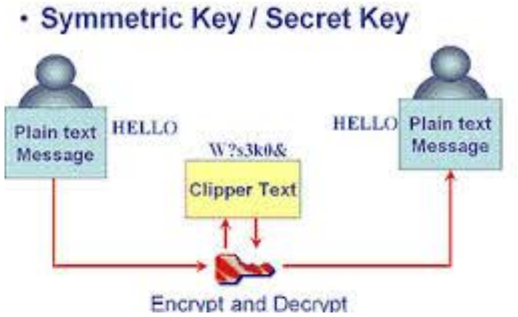

**Figure:**-symmetric key cryptography

Note that the symmetric key encryption uses a single key(the key itself may be a set of values) for both encryption and decryption. In addition, the encryption and decryption algorithm are inverses of each other. If P is the plaintext, C is the ciphertext, and k is the key, the encryption algorithm Ek(x) creates the ciphertext from the plaintext; the decryption algorithm Dk(x) creates the plaintext form the ciphertext. It is assumed that Ek(x) and Dk(x) are inverses of each other. They cancel the effect of each other if they are applied one after the other on the same input. [1]

Encryption : $C = Ek(P)$
Decryption : $P = Dk(C)$
In which, $Dk(Ek(x)) = Ek(Dk(x)) = x$ ....(1.1)

The popular modern symmetric key cryptography are
1. Data Encryption Standard (DES)
2. Advanced Encryption Standard (AES)

The following sections describe the mathematics behind the asymmetric key cryptography.

**Groups** A group (G) is a set of elements with a binary operation•that satisfies four properties (or axioms) [1]. A commutative group, also called an abelian group if a group in which operator satisfies the four properties for group plus an extra property, commutative.
The four properties for group plus commutative are defined as follows:

**Closure:** If a and b are elements of G, then c=a•b is also element of G.

**Associativity:** If a,b and c are elements of G, then (a•b)•c = a•(b•c)

**Commutativity:** For all a and b in G, we have a•b=b•a.

**Existence of identity:** For all a in G, there exists an element e called the identity element such that e•a=a•e=a

### C . Digital signature algorithm

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reasonto believe that the message was created by aknownsender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. To create RSA signature keys, generate an RSA key pair containing a modulus N that is the product of two large primes, along with integers e and d such that e×d ≡ 1(mod □(N)), where □ is the Euler phi-function. The signer's public key consists of N and e, and the signer's secret key contains d. To sign a message m, the signer computes σ ≡ md(modN). To verify, the receiver checks that σe ≡ m(modN). To prevent attacks, one can first apply a cryptographic hash function to the message m and then apply the RSA algorithm described above to the result. This approach can be proven secure in the so-called random oracle model. Most early signature schemes were of similar type: they involve the use of a trapdoor permutation, such as the RSA function, or in the case of the Rabin signature scheme, computing square modulo composite n.

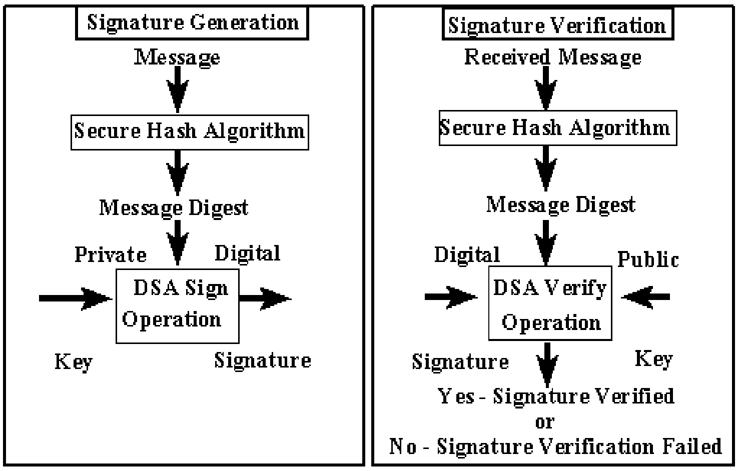

**figure:** geneation and creation of digital signature.

A trapdoor permutation is a family of permutations, specified by a parameter, that is easy to compute in the forward direction, but is difficult to compute in the reverse direction without knowing the private key. However, for every parameter there is a trapdoor (private key) which when known, easily decrypts the message. Trapdoor permutations can be viewed as public-key encryption systems, where the parameter is the public key and the trapdoor is the secret key, and where encrypting corresponds to computing the forward direction of the permutation, while decrypting corresponds to the reverse direction. Trapdoor permutations can also be viewed as digital signature schemes, where computing the reverse direction with the secret key is thought of as signing, and computing the forward direction is done to verify signatures. Because of this correspondence, digital signatures are often described as based on public-key cryptosystems, where signing is equivalent to decryption and verification is equivalent to encryption, but this is not the only way digital signatures are computed.

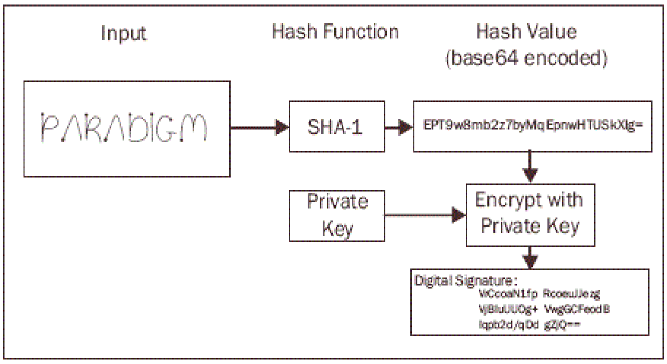

**Figure:** creating digital signature

### D. Blind signature

Sometimes we have a document that we want to get signed without revealing the contents of the document to the signer. David Chaum has developed some patented blind
Digital signature schemes for this purpose. The main idea is as follows:
1. Bob creates a blind message and sends to Alice.
2. Alice signs the blinded message and returned the signature on the blinded message.
3. Bob unblinds the signature to obtain a signature on the original message.

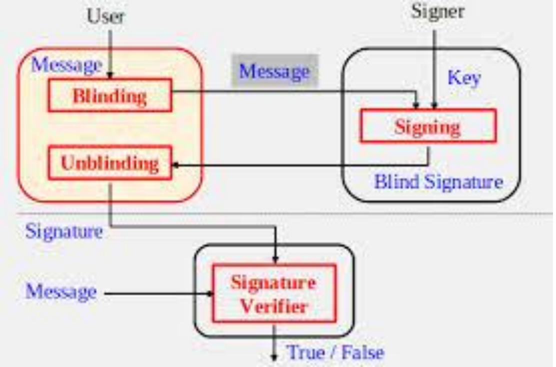

**Figure:** Blind signature

**Blind signature based on the RSA scheme:** Let us briefly describe a blind digital signature scheme developed by David Chaum. Blinding can be done using a variation of the RSA scheme. Bob selects a random number b and calculates the blinded message B = M×bemodn where e is Alice's public key and n is the modulus defined in RSA digital signature scheme. Here b can be called a blinding factor. Bob sends B to Alice. Alice signs the blinded message using the signing algorithm defined in the RSA.

### E. Problem statement

Keeping the research directions in view, it has been realised that there exists enough scope to implement elliptic curve in different areas of cryptography. Though elliptic curve cryptography is mainly used to key exchange process, our goal is to implement digital signature algorithm using elliptic curve cryptography. In particular, the objectives are narrowed to the use of proxy blind signature in elliptic curve cryptography. This proxy blind signature has already been implemented using elliptic curve cryptography. From here we conceived the idea of implementing it on elliptic curve.

## II. Literature Review

### A. Parallel Coprocessor Design for Genus-2

Hardware accelerators are often used in cryptographic applications for speeding up the highly arithmetic intensive public key primitives, e.g. in high-end smart cards. The emerging and very promising public key scheme is based on Elliptic Curve Cryptosystems (ECC). Optimal Tower Fields for HECC
Since the development of asymmetric cryptosystems based on elliptic and elliptic curves, it has been a challenging task to implement ECC and HECC over fields of odd characteristic.

**C. Optimal Tower Fields for ECC**

Since the development of asymmetric cryptosystems based on elliptic and elliptic cuves, it has been a challenging task to implement ECC and HECC over fields of odd characteristic.

## III. Arithematics Of Elliptical Curve

The elliptic curves, which can be seen as a generalization of elliptic curves. In the applications, group elements must be stored and transmitted. For restricted environments or restricted bandwidth it might be useful to use compression even though recovering the original coordinates needs some efforts. The main emphasis of this chapter is put on the arithmetic properties, i.e., on algorithms to perform the group operation. For cryptographic purposes on imaginary quadratic elliptic curves given by an equation 3.1.

$C : y2 + h(x)y = f(x),$
$h,f \in K[x],$
$\deg(f) = 2g + 1,$ .... (3.1)
$\deg(h) \leq g, f$ moni

This equation is elliptic curve of genus g over K if no point on the curve over the algebraic closure K of K satisfies both partial derivatives 2y + h = 0 and f0−h0y = 0. The last condition ensures that the curve is nonsingular. The negative of a point P = (x,y) is given by −P = (x,−y − h(x)). The points fixed under this elliptic involution are called Weierstraβ points. Elliptic curves are subsumed under this definition as curves of genus one [4].

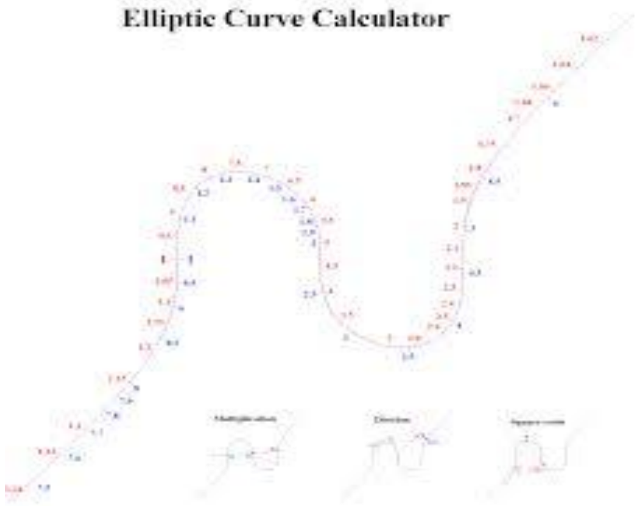

**Figure:** calulation of elliptical curve cryptography

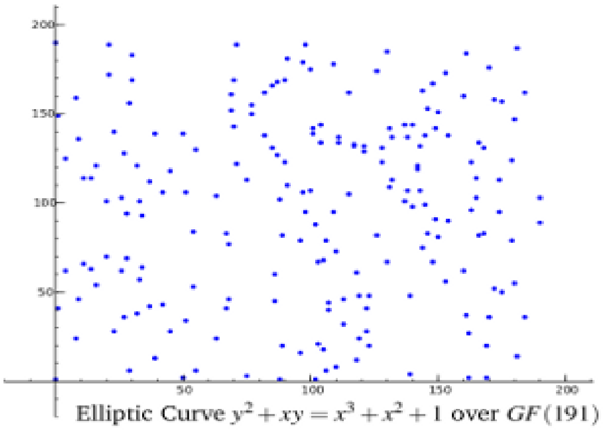

**Figure:** elliptical curve equation

### A. Group Laws for elliptic curves

For elliptic curves one can take the set of points together with a point at infinity as a group. For curves of genus larger than one this is no longer possible. The way out is to take finite sums of points as group elements and perform the addition coefficient-wise like (P +Q)⨁(R+Q) = P +2Q+R.

### B. Divisor class group and ideal class group

The group we described so far is called the divisor class group Pic0 cof C. To formally define the group law we need to take into account a further point P∞ called the point at infinity. Let C be a elliptic curve of genus g over K given by an equation of the form. The group of divisors of C of degree 0 is given by equation 3.2

Div0 c = {D =X P∈C
npP | np ∈Z, np = 0 for all most all P ∈ C,
X P∈C
np = 0, and such that σ(D) = D for all σ ∈ Gk} ....(3.2)

This latter condition means that the divisor is defined over K. This is equivalent to nσ(P) = nP for all σ ∈ GK, the Galois group of K.The divisor class group Pic0 c of C is the quotient group of Div0 c by the group of principal divisors, that are divisors of degree zero resulting from functions [4].
Each divisor class can be uniquely represented by a finite sum as given in equation 3.3

r X i=1
Pi −rP∞,PiC{P∞},r ≤ g .... (3.3)

Where for i 6= j we have Pi = (xi,yi) 6= (xj,−yj −h(xj)) = −Pj.
The following introduces a different representation that is more useful for implementations, and for which one can simply read off the field of definition of the group elements. Mumford representation makes explicit this isomorphism and we will use the representation as an ideal class group for the arithmetic. To fix names we keep speaking of the divisor class group and call the group elements divisor classes even when using the notation as ideal classes.

### Mumford representation

Let C be a genus g elliptic curve given by C : y2 + h(x)y = f(x), where h,f ∈ K[x], deg f = 2g + 1, deg h ≤ g. Each nontrivial divisor class over K can be represented via a unique pair of polynomials u(x) and v(x),u,v ∈ K[x] , where

1. u is monic,
2. deg v < deg u ≤ g,
3. u | v2 + vhf Let D =Pr i=1 Pi −rP∞, where Pi 6= P∞, Pi 6= −Pj for i 6= j and r ≤ g. Put Pi = (xi,yi). Then the divisor class of D is represented by equation 3.4

u(x) =r Y i=1 (x−xi) .... (3.4)

A divisor with at most g points in the support satisfying Pi 6= P∞, Pi 6= −Pj for i 6= j is called a reduced divisor. The first part states that each class can be represented by a reduced divisor.

### Cantor’s algorithm

**Input:** Two divisor classes ¯ D1 = [u1,v1] and ¯ D2 = [u2,v2] on the curve C : y2 + h(x)y = f(x)

**Output:** The unique reduced divisor D such that ¯ D = ¯ D1 ⨁ D2 initialization
1. d1 ← gcd(u1,u2) [d1 = e1u1 + e2u2]
2. d ← gcd(d1,v1 + v2 + h) [d = c1d1 + c2(v1 + v2 + h)]
3. s1 ← c1e1, s2 ← c1e2 and s3 ← c2
4. u ← u1u2 d2 and v ← s1u1v2+s2u2v1+s(v1v2+f) d mod u
5. Repeat
6. u’← f−vh−v2 u and v0 ← (−h−v) mod u0 .. u← u0 and v ←0
7. Untill deg u ≤ g
8. make u monic

9. return [u,v]

## IV. Blind Signature Scheme Using Elliptical Curve Cryptography

D. Chaum introduced the concept of a blind signature scheme in 1982. An use.A can obtain the signature of B by using this scheme on any given message, without revealing any in formation about the message or its signature. Apart from unforgeability, the scheme ensures untraceability and unlinkability. A lot of work has been done in field of blind signature schemes since Chaum. For example, in production of coins, the user makes the bank blindly sign a coin using blind signature schemes. The user is in possession of a valid coin such that the bank itself cannot recognize nor link with the user. Whenever a user goes through a valid branch to withdraw a coin, he needs the branch to make proxy blind signature on behalf of the signee bank. This application leads to the need of blind signature schemes [5].

### A. Proposed scheme: blind signature

In this section we have presented our proposed scheme. This scheme is based on elliptic curve cryptography and proxy blind signature. The proposed scheme is depicted as follows. Let a elliptic curve C of genus g be defined over field Fq of finite order defined by equation 4.1

$y2 + h(x)y = f(x) \bmod q$ ....(4.1)

Where h(x)is a polynamial and degree of h(x) ≤ g and f(x) is a monic polynamial of degree ≤ 2g + 1. The divisor D is defined as follows: D =XmiPi (4.2) is a formal weighted sum of points Pi of the curve C (and the integers mi are the wights) A reduced divisor can be represented as a pair of polynomials{u(x),v(x)}. Reduced divisors can be added (group addition). e.g. D3 = D1 + D2, or doubled (group doubling), e.g. D2 = 2D1 = D1 + D1 , and hence the scalar multiplication kD = D +...+ D for k times is defined. The scalar multiplication kD is the basic operation of HECC.

Parameter initialization
A = Sender Alice
B = Receiver Bob
P = a large prime number
q = large prime factor of (p-1)
g = an element of Z∗ p of order q
xA = secret key of original signer A
yA = public key of A = xAD
D = Divisor

**Proxy phase:**

1.**Proxy generation**: The original signer A randomly chooses k ∈ Z∗ q, k 6= 1
R = kD
S = xA + k.[D]x
Yp = S.D .... (4.3)

2. **Proxy delivery:** The original signer sends (S,R) to a proxy signer B in a secure way. And makes YP public.

3. **Proxy verification:**After receiving the secret key (S,R) the proxy signer B checks the validity of the secret key with the following equation

YP = yA + [D]x ·R ....(4.4)

Proof:
YP = S.D
= (xA + k[D]x)D
= xAD + k[D]xD
= yA + [D]xR
If received (S,R) satisfies the equation 4.4 then B accepts it as valid signature.

**Signing phase**

1. B chose random number k1 ∈ Z∗ q such that k1 6= 1 compute: RB = k1D Now B sends RB to C
2. C chooses randomly α,β ∈ Z∗ q Rc = RB k βYp If Rc = 0 choose another set of α,β else ec=H(r,m) e=ec+β

C sends e to B
3. B computes S’=k1 −Se B sends S’ to C
4. C computes Sp = S0 + α
The blind signature is (m,Sp,ec)

**Varibcaion:**
Recipient of the proxy blind signature computes e, =h(SpD k ecYP k M) Where YP is the public value. Check e, = ec If and this statement true then tuple(m,SP,ec) is a valid proxy signature.

**B. Security Analysis**
Elliptic curve cryptography is used as the fundamental scheme for this research. The elliptic curve cryptography is more secure than elliptic curve cryptography. It with stand many cryptographic attack. Therefore the security analysis of proxy blind signature is described in following section.

**1.** A different equation has been used for checking of original signatures and the proxy signatures in our proposed scheme. Thus original signature is distinguishable from the proxy signature.

**2**. In our scheme to put a valid proxy signature S (in case proxy protected xB too) is needed. Without knowing XB or S or both this is impossible to create a valid signature. This is the reason why proxy signature cannot be forged. Furthermore, original signer have no knowledge about xB though he creates S in case of proxy protected scheme. Hence the proxy signer cannot deny later that the proxy signature not created by him.
**3.** The public key YP has been calculated from the original signers public key yA. Hence the original signer cannot deny his agreement later. The public key of Proxy signer is also involved in the public key (in case proxy protected). Therefore the proxy signer can be identified from the signature.

## V. Conclusion

In this thesis we have proposed the proxy blind signature based on elliptic curve cryptography. Three phases, namely phase, signing phase, varification phase are there in our proposed scheme. In proxy phase the proxy is generated and delivered. In signing phase the signature obtained from previous phase is used to sign. In third phase which is called varification phase, the obtained blind is varified. All these techniques are implemented over elliptic curve cryptography. HECC uses minimum key size less than ECC. This is more suitable than ECC in Resource constraint environments.

## References

[1]. Behrouz A Forouzan. Cryptography & Network Security. McGraw-Hill, Inc., 2007.
[2]. J. Pelzl, T. Wollinger, and C. Paar. High performance arithmetic for special elliptic curve cryptosystems of genus two. In International Conference on Information Technology: Coding Computing, ITCC, volume 2, pages 513–517, 2004.
[3]. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, “Rotation, scale, and translation resilient public watermarking for images,” IEEE Trans. Image Process., vol. 10, no. 5, pp. 767-782, May 2001.
[4]. Henri Cohen. Handbook of Elliptic and elliptic Curve Cryptography. CRC Press, Abingdon, 2005
[5]. Sunder Lal and Amit K Awasthi. Proxy blind signature scheme. 2003.
[6]. Masahiro Mambo, Keisuke Usuda, and Eiji Okamoto. Proxy signatures for delegating signing operation. In Proceedings of the 3rd ACM conference on Computer and communications security, pages 48–57. ACM, 1996.
[7]. Seungjoo Kim, Sangjoon Park, and Dongho Won. Proxy signatures, revisited. Information and Communications Security, pages 223–232, 1997.
[8]. L. You and Y. . Sang. Effective generalized equations of secure elliptic curve digital signature algorithms. Journal of China Universities of Posts and Telecommunications, 17(2):100–108+115, 2010.
[9]. L. You and Y. . Sang. Effective generalized equations of secure elliptic curve digital signature algorithms. Journal of China Universities of Posts and Telecommunications, 17(2):100–108+115, 2010.
[10]. G. Bertoni, L. Breveglieri, T. Wollinger, and C. Paar. Finding optimum parallel coprocessor design for genus 2 elliptic curve cryptosystems. In International Conference on Information Technology: Coding Computing, ITCC, volume 2, pages 538–544, 2004
[11]. X. Fan and Y. Wang. Simultaneous divisor class addition-subtraction algorithm and its applications to elliptic curve cryptosystem. In Proceedings - International Conference on Advanced Information Networking and Applications, AINA, volume 1, pages 978–983, 2005.
[12]. ] T. Wollinger, J. Pelzl, and C. Paar. Cantor versus harley: Optimization and analysis of explicit formulae for elliptic curve cryptosystems. IEEE Transactions on Computers, 54(7):861–872, 2005
[13]. T. Wollinger and V. Kovtun. Fast explicit formulae for genus 2 elliptic curves using projective coordinates. In Proceedings - International Conference on Information Technology-New Generations, ITNG 2007, pages 893–897, 2007
[14]. Z. Zemao, Z. Zhijin, T. Xianghong, and L. Yichun. A new id-based blind signature from bilinear pairings. In IET Conference Publications, page 403, 2006.
[15]. R. Ganesan and K. Vivekanandan. A novel hybrid security model for e-commerce channel. In ARTCom 2009 - International Conference on Advances in Recent Technologies in Communication and Computing, pages 293–296, 2009.
[16]. T. J. Park, M. . Lee, K. Park, and K. Chung II. Speeding up scalar multiplication in genus 2 elliptic curves with efficient endomorphisms. ETRI Journal, 27(5):617–627, 2005.

[17]. P. Gaudry, D. Kohel, and B. Smith. Counting points on genus 2 curves with real multiplication, volume 7073 LNCS of Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2011

[18]. Schrder and D. Unruh. Security of blind signatures revisited, volume 7293 LNCS of Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2012.

[19]. I-Te Chen, Ming-Hsin Chang, and Yi-Shiung Yeh. Design of proxy signature in the digital signature algorithm (dsa). J. Inf. Sci. Eng., 22(4):965–973, 2006.

[20]. T. Wollinger and C. Paar. Hardware architectures proposed for cryptosystems based on elliptic curves. In Proceedings of the IEEE International Conference on Electronics, Circuits, and Systems, volume 3, pages 1159–1162, 2002.